La liberté à l'ère numérique

François Pellegrini

La liberté à l'ère numérique

François Pellegrini

Université de Bordeaux, LaBRI & Inria Bordeaux - Sud-Ouest, 351 cours de la Libération, 33405 Talence cedex, France. francois.pellegrini@labri.fr

I.– Liberté et libertés

La liberté peut être définie succinctement comme l'aptitude des individus à exercer leur volonté. Le droit des personnes à la liberté a été reconnu et formalisé au sein des sociétés modernes par la garantie d'un ensemble de libertés individuelles et collectives, telles que les libertés de circulation, de parole, de culte, d'association, de la presse, etc., étant entendu que l'exercice par chacun de ses libertés ne doit pas causer un préjudice injustifié à autrui [1]. Ces libertés ont parfois été exprimées sous forme de droits positifs, tels que le « droit à la vie privée » [2].

Exercer l'autonomie de sa volonté suppose, d'une part, l'absence de contraintes effectives à agir et, d'autre part, une information préalable suffisante et loyale. De fait, la réduction de l'asymétrie de l'information sous-tend de nombreux droits et libertés : liberté d'expression, liberté de la presse, droit à communication des documents administratifs, des données personnelles, des pièces d'accusation, etc.

L'ouverture des espaces numériques offre de nouvelles possibilités d'exercer ses libertés. Comme l'a énoncé avec humour Peter STEINER dans son célèbre *cartoon* de 1993 figurant un labrador assis derrière son ordinateur de bureau : « *On the Internet, nobody knows you're a dog* ». Ainsi la révolution numérique transforme-t-elle profondément les rapports sociaux, par exemple en permettant la mise en relation directe de personnes partageant les mêmes centres d'intérêts, ou encore, grâce au pseudonymat rendu possible sur de nombreuses plates-formes, en permettant aux personnes de se forger une ou plusieurs identités numériques potentiellement décorrélées de leur apparence physique et de leur réalité sociale. Cependant, dans le même temps, la généralisation des échanges numériques fait peser un risque nouveau sur les personnes, en exacerbant le risque d'asymétrie au profit de ceux capables de traiter les masses considérables d'informations et de traces collectées par ces plates-formes.

L'ouverture des espaces numériques a naturellement conduit le législateur à y étendre son pouvoir de régulation. La loi pénale étant d'interprétation stricte, il a fallu définir de nouvelles incriminations pour les délits spécifiques au monde numérique. Tel est par exemple le cas de la loi « Godfrain » du 5 janvier 1988 relative à la fraude informatique, destinée à réprimer l'intrusion dans les systèmes de traitement automatisés de données (STAD) et la manipulation des données qu'ils hébergent. En dépit de tentatives malheureuses de la part de certains tribunaux, ces délits ne peuvent en effet aucunement être réprimés par les articles sanctionnant la violation de domicile ou le vol. Il est en effet inconcevable d'accuser une personne étant restée derrière son ordinateur d'être entrée chez une autre, tout comme d'assimiler la copie illicite de données à du vol. En effet, le vol est défini comme la « soustraction frauduleuse de la chose d'autrui » à son propriétaire. Or, la copie illicite de données ne peut aucunement être considérée comme une soustraction, tout comme les données, en tant que biens non rivaux, ne peuvent avoir de propriétaire [3].

Comme pour les bouleversements antérieurs tels que l'imprimerie, définir le point d'équilibre de la loi nécessite la compréhension des principes de l'informatique tant par le législateur que par la société au sens le plus large. Ce débat ne peut être une affaire de spécialistes, et la question du rapport entre numérique et liberté concerne l'ensemble de la société. Il s'agit d'une responsabilité collective, caractérisée par la prise de position d'instances représentatives de la communauté dans le débat public. La communauté scientifique participe à son introspection, par la mise en place de comités d'éthique [4], etc. Il s'agit également d'une responsabilité individuelle. C'est à ce titre que plusieurs personnes ont fait le choix de la dissidence, telles Edward Snowden. Il est d'ailleurs à remarquer qu'Edward Snowden n'était pas un opérationnel de la NSA, mais un administrateur système, mettant en œuvre des fonctions de support. À l'image du personnel de ménage disposant de l'ensemble des clés d'accès à une entreprise, les techniciens informatiques disposent souvent des privilèges les plus étendus.

1. Article 4 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789 : « La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres Membres de la Société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la Loi. »

2. Ce dernier est d'expression récente, puisqu'il n'a été intégré dans le droit positif qu'en 1948, consacrant l'individualisme de la société occidentale moderne.

3. En effet, une même donnée peut être produite de façon indépendante par des acteurs ne se connaissant pas. Cette évidence intellectuelle n'empêche pas certains tribunaux, aiguillonnés par la volonté de réprimer un comportement considéré comme répréhensible en dépit de l'absence d'une base légale adéquate, de passer outre le principe d'interprétation stricte de la loi pénale. Voir par exemple : C.A. Paris, ch. 4-10, 5 février 2014, puis C. Cass., ch. crim. n° 1566, 20 mai 2015.

4. C'est le cas d'Allistene dans le domaine des sciences du numérique.

II.– Régulation des traitements algorithmiques

L'accroissement des capacités de traitement de masses de données de plus en plus considérables a fait émerger dans le débat public la notion d'« algorithme », terme souvent nimbé de magie. Cette apparition d'un terme supposé nouveau, ou tout du moins appliqué à une situation nouvelle, a pu faire s'interroger une partie de la communauté juridique sur la nécessité de « réguler les algorithmes » pour préserver les libertés des personnes. La réponse est double : elle consiste, d'une part, à refuser le mésusage de ce terme et, d'autre part, à étendre ce questionnement à l'ensemble des cas d'usage des traitements algorithmiques.

A.– Statut juridique des traitements algorithmiques

Débattre du statut des « algorithmes » nécessite de préciser de quoi il est effectivement question. Les algorithmes (sans guillemets) sont la description d'une suite d'étapes permettant d'obtenir un résultat à partir d'éléments fournis en entrée [5]. Ce sont des constructions mathématiques purement abstraites, conçues pour répondre à un problème scientifique ou technique. De par leur nature mathématique, ils appartiennent au fonds commun des idées [6] et ne sont donc en droit susceptibles d'aucune monopolisation d'usage, conformément au principe que « les idées sont de libre parcours » [7]. Pour autant, du fait des bénéfices économiques inhérents à la création d'innovations algorithmiques, il existe une forte pression d'acteurs privés pour créer des monopoles dans ce domaine. C'est ainsi que de nombreux offices de brevets prônent (et agissent parfois également de façon illégale) pour faire autoriser par le législateur l'existence de brevets sur les méthodes algorithmiques, improprement appelés « brevets logiciels », qui correspondent en fait à la possibilité de monopoliser un savoir mathématique [8]. Les brevets de ce type sont contestés, y compris aux États-Unis, non seulement du fait de leur toxicité macro-économique sur l'innovation, mais aussi parce qu'ils portent atteinte de façon disproportionnée à la liberté d'expression.

Les algorithmes sont consubstantiels de l'apparition de la pensée humaine, mais il a fallu l'invention des ordinateurs pour permettre leur application mécanisée à de grandes masses de données. Pour cela, il est nécessaire d'exprimer les algorithmes que l'on souhaite mettre en œuvre, sous la forme d'un « programme d'ordinateur » ou « logiciel » [9]. Cette création de forme est protégée par le droit d'auteur adapté, qui diffère du droit d'auteur classique par un certain nombre d'amodiations découlant de la double nature, à la fois artisanale et utilitaire, de ces biens [10].

Un logiciel n'est que du « code mort ». Pour qu'il prenne vie, il faut qu'il soit mis en œuvre au sein d'un environnement informatique, constitué d'un ordinateur connecté à des périphériques d'entrée (pour l'acquisition des informations provenant du monde extérieur) et de sortie (pour restituer les résultats des traitements opérés et éventuellement agir directement sur l'environnement). Le processus qui s'exécute effectivement peut être soumis à des aléas et erreurs transitoires issues de l'environnement. L'objet juridique correspondant est le « traitement de données », déjà défini dans la loi, tant en ce qui concerne les données personnelles (c'est le cœur de la loi « Informatique et Libertés » du 6 janvier 1978) que les données non personnelles (comme avec la loi « Godfrain » sur les STAD). Les « responsables de traitement » sont, *in fine*, responsables de la bonne mise en œuvre dudit traitement et du respect des droits des personnes concernées, sur les plans contractuel et légal.

L'encadrement juridique du monde des « algorithmes » est donc déjà largement établi. Les questions débattues actuellement portent en fait majoritairement sur l'encadrement des relations économiques entre les responsables de traitement et les usagers de ceux-ci.

B.– Loyauté des traitements

Tel est le cas de la « loyauté », qui ne concerne absolument pas les « algorithmes » en tant que constructions mathématiques. Il s'agit en l'espèce de définir les règles applicables aux responsables de traitements qui, en fonction de leur mise en œuvre logicielle et de leurs relations économiques avec des tiers, pourraient choisir de rendre un service déloyal ou inéquitable à leurs usagers (comme par exemple de calculer un itinéraire passant devant le plus de panneaux publicitaires possible).

Tel est également celui de la « transparence ». Il semble naturel d'informer les usagers sur la nature du traitement opéré sur leur données, et des tiers avec lesquels le responsable de traitement est en relation commerciale dans le cadre dudit traitement. Cependant, dans le cas des algorithmes auto-apprenants, la connaissance des principes algorithmiques mis en œuvre importe moins que la nature du jeu de données qui a servi à entraîner cet algorithme dans le contexte spécifique du traitement en question. C'est du choix de ce jeu de données que découlera l'existence potentielle de biais qui, en pénalisant silencieusement certaines catégories de personnes, détruiraient l'équité supposée du traitement.

5. Voir par exemple la définition qu'en donne la CNIL : https://www.cnil.fr/fr/definition/algorithme .
6. François PELLEGRINI, « L'originalité des œuvres logicielles », *Revue internationale du droit d'auteur*, avril 2017, pp. 45-105.
7. Henri DESBOIS, *Le droit d'auteur en France*, 3e éd., Dalloz, 1978, p. 22.
8. François PELLEGRINI et Sébastien CANEVET, *Droit des logiciels*, Puf, 2013, § 353 et s.
9. Ces deux termes sont parfaitement équivalents en l'état de la technique. Ce n'est qu'avant la mise au point des architectures de type « von Neumann », au tout début de l'informatique moderne, qu'il pouvait exister des programmes d'ordinateurs qui ne soient pas des logiciels. Il s'agissait de programmes câblés « à la main » sur les tableaux de commande, au moyen de fiches, câbles et connecteurs. Les logiciels, pour leur part, sont immatériels et de ce fait pleinement soumis à l'économie des biens non rivaux.
10. François PELLEGRINI et Sébastien CANEVET, Op. cit., § 114 et s.

L'assimilation du code source des logiciels de l'administration à un document administratif, communicable au titre de la loi « CADA » du 17 juillet 1978 instituant la Commission d'accès aux documents administratifs, participe à l'information des personnes concernées [11], de même que l'obligation d'informer sur la nature des traitements instaurée par la loi « République numérique » du 7 octobre 2016 en ce qui concerne les traitements mis en œuvre par la puissance publique [12] ; il convient que cette obligation soit étendue au secteur privé. La description fonctionnelle abstraite des traitements n'est pas de nature à porter atteinte au secret industriel, et rassurerait les usagers quant à la loyauté des traitements et l'éthique de leurs responsables.

Pour autant, quelle capacité effective les usagers ou les autorités de contrôle ont-elles pour déterminer si un dispositif est loyal ou non ? La décompilation d'un logiciel, pour en comprendre les principes, n'est en effet autorisée qu'à fin d'interopérabilité ou de sécurité et non, par exemple, pour la vérification du respect des normes anti-pollution. Comment l'usager peut-il s'assurer qu'un logiciel ne possède pas de « portes dérobées » [13] permettant à des tiers d'accéder à ses données (voir *infra* en ce qui concerne la cryptographie) ? De nombreux dispositifs et logiciels sont également protégés par des « verrous numériques » et autres barrières technologiques qui empêchent d'en étudier le fonctionnement.

Plus largement, ces verrous numériques interfèrent avec la liberté d'usage d'un bien, étant utilisés pour maintenir des marchés captifs sur la maintenance et empêcher les usagers de configurer leurs outils selon leurs besoins [14]. Les constructeurs découragent également toute manipulation des biens par les usagers, en arguant que toute modification conduira à l'annulation de la garantie qu'ils offrent.

C.– Loyauté du réseau

Les algorithmes, protocoles et traitements mis en œuvre pour gérer les réseaux numériques définissent les capacités et modalités d'accès aux ressources atteignables à travers ces réseaux. Les questions d'équité d'accès et de circulation de l'information au sein des réseaux sont abordées de façon globale à travers la notion de « neutralité » [15]. Celle-ci pose le principe de non-discrimination du trafic circulant sur le réseau, quels que soient la source, la destination, le protocole ou le contenu transmis [16]. Ainsi, selon le principe de neutralité, le réseau doit-il être loyal vis-à-vis de l'ensemble de ses usagers. Ce principe est essentiel à l'équité d'accès à l'Internet, réseau public ayant vocation à interconnecter tous ceux qui souhaitent l'être, à l'image du réseau routier.

La neutralité des réseaux prolonge dans l'espace numérique la liberté de parole. Elle lui est en fait supérieure, car là où la liberté de parole ne garantit que la possibilité pour le locuteur d'émettre, la neutralité des réseaux lui garantit celle de pouvoir être entendu de tous.

Les principes fondateurs de l'Internet devant être respectés de façon collective pour être effectifs, sa gouvernance est devenue un enjeu mondial. Cette question, dont se sont saisies les Nations unies au début du siècle [17], est encore largement ouverte, tant les différents acteurs en présence expriment des positions divergentes : États (ceux-ci n'ayant pas une position homogène, les intérêts des États-Unis d'Amérique n'étant pas réductibles à ceux de l'Union européenne, de la Chine, de la Russie, du Brésil ou encore de l'Iran), secteur privé (les multinationales des télécommunications n'ayant pas non plus les mêmes intérêts que les grandes plate-formes de contenu), société civile, monde académique [18]. Derrière des questions apparemment techniques telles que les protocoles de résolution de noms de domaine (DNS, pour « Domain Name System ») ou de routage, s'expriment en fait des enjeux stratégiques considérables : le contrôle sur les serveurs de noms de domaines permet de « faire disparaître » des pays entiers de l'Internet, et la capacité d'influer sur le routage du trafic permet par exemple de rediriger le trafic intra-européen vers des nœuds du réseau situés dans des zones géographiques où se pratiquent la collecte indiscriminée du trafic et la surveillance de masse.

D.– Responsabilité des systèmes autonomes

L'accroissement des puissances de traitement et l'avancée des méthodes informatiques (traitements auto-apprenants, réseaux de neurones multi-niveaux, etc.) permettent de confier des fonctions de contrôle de plus en plus élaborées à

11. Voir en ce sens l'avis CADA n° 20144578, séance du 8 janvier 2015, http://www.cada.fr/avis-20144578,20144578.html ; puis T.A. Paris, 5ème section – 2ème chambre, n° 1508951/5-2, 10 mars 2016, https://cdn2.nextinpact.com/medias/ta-dgfip.pdf, cité par : Xavier BERNE, « Le code source d'un logiciel, document administratif communicable au citoyen », NextInpact, 14 mars 2016, https://www.nextinpact.com/news/99038-la-justice-confirme-qu-un-code-source-logiciel-est-document-administratif-communicable-au-citoyen.htm .

12. Article L. 311-3-1 du code des relations entre le public et l'administration.

13. Une porte dérobée est une fonctionnalité logicielle, inconnue de l'administrateur d'un système informatique, et qui permet d'acquérir des privilèges et / ou d'effectuer des actions que cet administrateur n'aurait pas autorisés. Voir *infra*.

14. Jason KOEBLER, « Right to Repair: Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware », *Motherboard / Vice.com*, 21 mars 2017, https://motherboard.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware .

15. Pour une vision d'ensemble des problématiques liées à la neutralité de l'Internet, voir : Luca BELLI et Primavera DE FILIPPI, eds., *Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet*, Springer, 2016, ISBN 978-3-319-26425-7.

16. Tim WU, « Network Neutrality, Broadband Discrimination », *Journal of Telecommunications and High Technology Law*, vol. 2, p. 141, 2003.

17. En 2003, puis 2005, fut organisé le Sommet mondial sur la société de l'information, forum intergouvernemental mondial organisé par l'Union internationale des télécommunications, une agence spécialisée de l'ONU.

18. Pour une étude exhaustive de ces questions, voir : Luca BELLI, *De la gouvernance à la régulation de l'Internet*, thèse de doctorat en droit public de l'université Paris II Panthéon-Assas, Berger-Levrault, Coll. *Au fil des études, Les thèses*, 2016.

des automatismes. Ces avancées rendent possibles des applications qui relevaient jusqu'il y a peu du domaine de la science-fiction, telles que les voitures ou les robots de combat autonomes.

Dans chacun de ces cas, l'autonomie recherchée de ces équipements fait que les personnes qui les mettent en œuvre n'ont qu'un contrôle partiel sur leur fonctionnement. Cela conduit à s'interroger sur la question de la responsabilité juridique en cas d'accident ou de « bavure », entre celle du concepteur qui fournit un produit pouvant être jugé comme défectueux et le responsable de la mise en œuvre de l'objet, susceptible d'être accusé d'usage non conforme.

Au delà, se pose plus largement la question de la liberté des usagers. Tout logiciel est un objet socio-économique, dont la conception et l'usage dépendent fortement de leur contexte culturel et économique. Un logiciel code donc par nature de la norme sociale. Le fait qu'un formulaire ne puisse proposer comme choix que « M. / Mme » manifeste le consensus social que seules ces deux réponses sont admissibles. De même, dans le cas du véhicule autonome, lorsqu'un piéton traverse devant le véhicule, celui-ci doit-il écraser le piéton et préserver la vie du conducteur, ou bien détourner le véhicule vers un mur qui risquerait de tuer son occupant ? Ces choix éthiques, expérimentés par PHILIPPA FOOT [19] et popularisés sous le terme générique de « dilemme du tramway » [20], sont à l'heure actuelle laissés sous l'entier contrôle du concepteur du logiciel de conduite du véhicule, l'occupant renonçant alors à la liberté de choix qu'il aurait en tant que conducteur manuel. La préservation de la liberté des personnes implique-t-elle la capacité de pouvoir paramétrer ces logiciels d'une façon spécifique au type d'occupant ? Plus généralement, est-il possible de modifier ces logiciels, au même titre que les autres logiciels embarqués ?

III.– Régulation des données

La maîtrise de son patrimoine informationnel peut se définir comme la liberté de gérer les données dont on est le responsable. Dans le monde numérique, cette gestion est déléguée à des intermédiaires techniques (fabricants d'ordinateurs et de réseaux, éditeurs de logiciels, responsables de traitements), ce qui pose ici encore la question de la liberté effective des personnes face à ces tiers, ainsi que face à la puissance publique susceptible de leur imposer en sus ses propres règles.

A.– Statut des données à caractère personnel

La puissance des outils numériques a considérablement accru les possibilités de fichage et de contrôle des populations. Alors que la mécanographie, héritée du XIXe siècle, ne permettait que des tris et des recherches sommaires au sein de fichiers déjà constitués, l'informatique moderne a permis les croisements et la recherche de corrélations entre des masses considérables de données. Dans les années 1970, l'informatisation des fichiers de personnes est considérée comme une opération de modernisation technique nécessaire et bénéfique pour une conduite moderne de l'État. Les conséquences funestes du fichage généralisé employé lors de la Seconde Guerre mondiale [21] ont néanmoins conduit au vote, en 1978, de la loi « Informatique et Libertés », qui crée la Commission nationale de l'informatique et des libertés (CNIL) et donne de nouveaux droits aux personnes fichées.

À l'époque de la création de la CNIL, seuls les États étaient en capacité de ficher massivement les personnes. Au tournant du millénaire, la démocratisation de l'Internet et le développement du commerce connecté ont conduit à un glissement apparent de cette menace vers le secteur privé. Les grandes entreprises gestionnaires de plate-formes de contenu (communément désignées sous le terme « GAFA », pour « Google - Apple - Facebook - Amazon ») ont alors commencé à disposer de capacités de stockage et de traitement supérieures à celles de bien des États mais, surtout, ont pu attirer à elles, grâce à leurs services, un volant d'usagers représentant une fraction significative de la population mondiale. Ce n'est que grâce à certaines fuites, dont la plus significative est due à Edward Snowden, que les programmes de collecte mondiale de données personnelles et de surveillance globale mis en œuvre par les États ont pu être révélés, remettant sur le devant de la scène le risque du mésusage de ces informations à l'encontre des populations.

Le périmètre des données concernées s'est sans cesse élargi, à mesure que la numérisation de la société et les progrès de la science informatique ont permis d'extraire des informations identifiantes de données qui jusqu'alors n'étaient pas considérées comme telles. Alors que la loi ne concernait initialement que les « informations nominatives », directement associées aux individus, la généralisation des identifiants numériques tels que numéros de téléphone ou de plaques d'immatriculation a conduit à étendre son champ aux « informations indirectement nominatives », permettant de retrouver une personne par simple consultation d'un index. Cependant, le nom n'est que l'une des caractéristiques d'une personne. C'est pourquoi, afin de prendre en compte l'intégralité des informations pouvant caractériser une personne, le périmètre de la loi a été étendu aux « données à caractère personnel », terme souvent abrégé en « données personnelles ». Sont ainsi couvertes toutes les catégories de données pouvant être rattachées directement ou indirectement aux personnes physiques, telles que la biométrie, les traces comportementales, les méta-données de connexions

19. Philippa Foot, « The Problem of Abortion and the Doctrine of the Double Effect », Virtues and Vices, Oxford, Basil Blackwell, 1978.
20. Judith Jarvis Thomson, « Killing, Letting Die, and the Trolley Problem », *The Monist*, vol. 59, 1976, pp. 204-217 ; Peter Unger, *Living High and Letting Die*, Oxford University Press, 1996.
21. Edwin BLACK, *IBM et l'holocauste*, Robert Laffont, Paris, 2001.

électroniques, les courbes de consommation électrique[22], etc. À ce titre, la collecte massive de données biométriques par les États, en dehors de tout cadre juridique et au mépris des conventions internationales visant à protéger les personnes contre l'immixtion dans leur vie privée, est extrêmement préoccupante. Cette « guerre de la biométrie » menée par les États contre les populations est symptomatique d'un basculement des sociétés qui, au prétexte d'une sécurité illusoire, placent l'ensemble des citoyens en situation de suspects à même de s'élever contre l'ordre établi[23].

Les risques liés à l'usage des outils numériques ont conduit à l'émergence de deux approches complémentaires visant à élever le niveau de protection des personnes. La première consiste à intégrer la prise en compte de la protection des données personnelles dès la phase de conception des systèmes informatiques (« *privacy by design* »). Elle repose sur un ensemble de méthodologies telles que la « minimisation des données », c'est-à-dire le fait de ne produire que les données strictement nécessaires au traitement projeté, et la mise en œuvre de principes architecturaux visant à réduire techniquement le risque de mésusage des données par des tiers en l'absence d'action positive des personnes. Il s'agira par exemple de conserver les données « à la main de l'usager »[24] et de distribuer les traitements auprès des personnes plutôt que de centraliser leurs données en vue d'un traitement global. La deuxième vise pour sa part à ce qu'un système informatique soit toujours initialement paramétré de façon à être le moins intrusif possible (« *privacy by default* »). Ces deux approches, élaborées dans la sphère nord-américaine[25], ont été consacrés en Europe par le Règlement général sur la protection des données personnelles[26].

Sur le plan du droit de la concurrence, le droit à la « portabilité des données » vis-à-vis des plate-formes d'hébergement a été consacré en France par la loi « République numérique ». Il constitue le prolongement, dans le monde des données personnelles et du « Saas » (« *Software as a Service* »), du droit à la décompilation à fin d'interopérabilité introduit dans le droit communautaire par la directive 91/250/CE.

B.– Statut de la cryptographie

La cryptographie constitue l'un des principaux moyens de garantir l'authenticité et de préserver la confidentialité des données, et tout particulièrement des données personnelles. Comme l'a confirmé Edward Snowden lors d'une de ses interviews : « *Le chiffrement fonctionne. Les crypto-systèmes robustes, mis en œuvre de façon appropriée, sont une des rares choses auxquelles vous pouvez vous fier*[27] ».

La cryptographie, de ce fait, constitue l'un des remparts des personnes contre l'arbitraire. Parce qu'elle peut être utilisée pour se protéger des pouvoirs d'investigation des forces de l'ordre, certains États, par la voie législative ou par des actions occultes[28], tentent avec constance de forcer cette protection.

Si un État répressif peut vouloir affaiblir et/ou interdire les outils cryptographiques de façon systématique, afin de garantir son pouvoir d'interception sur l'ensemble des communications et stockages numériques des citoyens, il doit en aller autrement d'un État démocratique. La puissance de l'informatique permet, si elle n'est pas contrôlée, la surveillance de masse à moindre coût de l'ensemble de la population. Le chiffrement de bout en bout des communications, depuis l'équipement de l'émetteur jusqu'à celui du destinataire, permet de rendre inopérante cette surveillance de masse ; seule est alors possible la surveillance ciblée, nécessitant de faire intrusion dans l'un des équipements terminaux afin d'intercepter le contenu des communications avant chiffrement et/ou après déchiffrement.

La lutte effective contre la surveillance de masse au moyen du chiffrement des communications et des espaces de stockage n'est effective qu'à plusieurs conditions. En premier lieu, il faut qu'il soit licite de l'utiliser. En second lieu, il faut que les outils utilisés soient efficaces, ce qui ne serait pas le cas s'ils étaient dotés de « portes dérobées ». D'une part, de telles failles à la main des États rendraient à nouveau possible la surveillance de masse et, d'autre part, la fuite de ces secrets constituerait un risque majeur pour l'ensemble de la société numérique, l'ensemble des transactions devenant accessibles à des personnes malveillantes. Cet argument plaide pour la plus grande liberté d'usage de la cryptographie, en autorisant les personnes à mettre en œuvre leurs propres méthodes et outils, et non les seuls outils qui seraient homologués par une agence. Outre que cela autorise et stimule la recherche et l'entrepreneuriat dans le secteur, la diversité de l'écosystème rend celui-ci plus résilient en cas de compromission de l'un des outils. En troisième lieu, il faut que l'usage de la cryptographie soit généralisé, par son activation par défaut au sein des outils

22. Il a été montré que l'analyse de la courbe de consommation électrique instantanée, aussi appelée « courbe de charge », pouvait permettre de déterminer les contenus visionnés par les personnes sur leurs téléviseurs. Ceci a conduit certaines autorités de protection des données à demander que les courbes de consommation énergétique soient fournies avec un pas de temps suffisamment long pour « diluer » ces informations dans une moyenne agrégée moins significative. Pour autant, cette moyenne permet encore de déterminer le nombre de personnes présentes dans l'habitation, par exemple. Voir : Ulrich GREVELER, Benjamin JUSTUS et Dennis LOEHR, « Multimedia content identification through smart meter power usage profiles », Computers, Privacy and Data Protection (CPDP), 2012.

23. François PELLEGRINI et André VITALIS, « Identités biométrisées et contrôle social », rapport de recherche Inria n° RR-9046, mars 2017, https://hal.inria.fr/hal-01492431v2 .

24. C'est le cas par exemple du stockage des données d'identification biométriques des personnes sur leurs badges individuels plutôt qu'au sein d'une base centralisée.

25. Ann CAVOUKIAN, *Privacy by Design — The 7 Foundational Principles*, IPC office, province d'Ontario, 2011, https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf .

26. Article 25 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE, http://eur-lex.europa.eu/legal-content/fr/TXT/PDF/?uri=CELEX:32016R0679 .

27. « *Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.* »

28. James BALL, Julian BORGER et Glenn GREENWALD, « Revealed: how US and UK spy agencies defeat internet privacy and security », *The Guardian*, 6 septembre 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security .

de communication, afin que ses usagers ne soient pas automatiquement considérés comme des suspects et ne fassent immédiatement l'objet d'une surveillance ciblée « de contrôle ».

C.– Identité, anonymat et ré-identification

L'anonymisation des données personnelles est essentielle à l'exercice des libertés. Il s'agit en l'espèce de préserver les aspects liés à la vie privée des personnes de fuites de données qu'elles ne souhaitent pas voir communiquées au public.

La protection contre la réassociation des personnes à leurs données est un problème ancien. Ainsi, par la loi du 7 juin 1951 « sur l'obligation, la coordination et le secret en matière de statistiques », fut créé au sein de l'INSEE un Comité du secret statistique. Il s'agissait alors de rassurer les entreprises et les particuliers, tous appelés à communiquer leurs données économétriques afin d'organiser la reconstruction du pays. Elle est également nécessaire au succès des démarches d'ouverture des données (« *open data* »), les responsables de traitements devant s'assurer que les données qu'ils ouvrent ne puissent conduire à la réidentification des personnes concernées.

Un premier niveau de protection, rudimentaire, consiste à décorréler l'identité des personnes des informations qui les concernent. Il ne s'agit pas d'une réelle anonymisation, mais d'une « pseudonymisation », qui n'offre pas toujours des garanties suffisantes. Par exemple, il est assez facile d'associer le plus haut revenu d'un petit village à la personne concernée. De façon plus inquiétante, des expériences récentes sur la ré-identification dans des masses de données ont pu montrer que quatre points de corrélation seulement étaient nécessaires pour identifier, à près de 90 %, une personne parmi une masse considérable de données pseudonymisées [29].

Face aux appétits que génèrent les traces comportementales pour le secteur marchand et les gouvernements, la liberté de circuler dans l'espace numérique est donc indissociable de la liberté d'usage des outils permettant d'y garantir l'anonymat, lesquels nécessitent le recours à une cryptographie loyale. Ces outils incluent les crypto-monnaies qui, tout comme l'argent liquide, permettent aux personnes d'effectuer des transactions sans que des tiers puissent en être informés.

La préservation des libertés est indissociable de l'émergence d'un droit à la « non-incrimination numérique ». Les personnes doivent avoir le droit de « garder le silence numérique », en particulier en échappant à l'obligation de fournir leurs identifiants de connexion, qui témoignent de l'ensemble des facettes de leur vie numérique, et a fortiori leurs mots de passe. Il s'agira de ne pas céder sur ces principes fondamentaux, actuellement mis à mal.

D.– Protection des lanceurs d'alerte

La question de la protection des personnes choisissant de dénoncer des comportements et actes répréhensibles déborde du strict cadre du numérique. Pour autant, elle est amplifiée par celui-ci, et comporte des aspects spécifiquement numériques, liés aux nouveaux modes de collecte et de diffusion des preuves.

Si les cadres actuellement mis en place au sein des entreprises et des administrations ont le mérite d'offrir une protection juridique dans certains cas, ils sont loin de résoudre globalement le problème. En effet, ils supposent une bienveillance de la puissance publique à l'égard des personnes concernées, qui n'est pas acquise dans tous les cas, que ce soit parce que l'État est incapable de fournir une protection efficace aux personnes concernées (dénonciation de réseaux mafieux) ou qu'il est lui-même impliqué dans les comportements dénoncés (surveillance de masse des populations).

La possibilité effective de laisser fuir des documents vers la presse et l'opinion publique suppose l'existence d'outils garantissant l'anonymat des sources. Ici encore, le recours à une cryptographie forte et loyale est une absolue nécessité, de même que la libre disposition et le libre usage d'outils de communication anonymes et résistants à la ré-identification.

Conclusion

La révolution numérique ne doit pas conduire à l'affaiblissement des droits fondamentaux existants, sous prétexte que cela est techniquement possible. Elle doit au contraire inciter à en étendre la préservation, d'une part, par la transposition au monde numérique des droits déjà garantis dans le monde physique et, d'autre part, par la sacralisation de nouveaux droits spécifiques à ce nouvel espace.

Si la préservation des droits fondamentaux prend sa source dans l'univers juridique, les considérations techniques n'en sont pas absentes. En particulier, l'architecture des systèmes d'information influe de façon déterminante sur leur robustesse et leur capacité à ne pas être détournés [30]. Ces éléments plaident en faveur de la nécessaire collaboration entre juristes et informaticiens pour maintenir le périmètre des libertés fondamentales.

29. Yves-Alexandre DE MONTJOYE, Laura RADAELLI, Vivek K. SINGH, Alex Sandy PENTLAND, « Unique in the shopping mall : On the reidentifiability of credit card metadata », Science 347 (6221), pp. 536-539. DOI 10.1126/science.1256297 (2015).

30. Thibaud ANTIGNAC et Daniel LE MÉTAYER, « Privacy by Design: From Technologies to Architectures », in *Privacy Technologies and Policy: Second Annual Privacy Forum*, APF 2014, Athènes, Grèce, 20-21 mai 2014, Springer International Publishing, pp. 1-17, DOI 10.1007/978-3-319-06749-0_1.